

Mail Stop: Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450



In re application of: **Tobias MARTIN et al.**  
Serial No.: 10/049,385  
Filed: 02/11/2002  
For: **METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS**

Sir:

Transmitted herewith is a **Supplemental Information Disclosure Statement (2 pages) with PTO-1449 (1 page) and cited references** in the above-identified application.

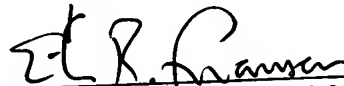
- ☐ Small entity status under 37 C.F.R. 1.9 and 1.27 has been previously established.  
☐ Applicants assert small entity status under 37 C.F.R. 1.9 and 1.27.  
☒ No fee for additional claims is required.  
☐ A filing fee for additional claims calculated as shown below, is required:

	(Col. 1)	(Col. 2)	
FOR:	REMAINING	HIGHEST	
	AFTER	PREVIOUSLY	PRESENT
	AMENDMENT	PAID FOR	EXTRA
TOTAL CLAIMS	* Minus 20	=	0
INDEP. CLAIMS	* Minus 3	=	0
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEP. CLAIM			

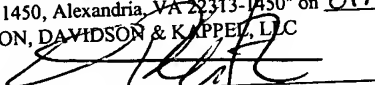
SMALL ENTITY		OR	LARGE ENTITY	
RATE	FEE		RATE	FEE
x \$ 25	\$		x \$ 50	\$
x \$ 100	\$		x \$ 200	\$
+ \$ 180	\$		+ \$ 360	\$
TOTAL: \$			TOTAL: \$	

- \* If the entry in Co. 1 is less than the entry in Col. 2, write "0" in Col. 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, write "20" in this space.  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, write "3" in this space.

- ☐ Also transmitted herewith are:  
☐ Petition for extension under 37 C.F.R. 1.136  
☐ Other:  
☐ Check(s) in the amount of \$0.00 is/are attached to cover:  
☐ Filing fee for additional claims under 37 C.F.R. 1.16  
☐ Petition fee for extension under 37 C.F.R. 1.136  
☐ Other:  
☒ The Assistant Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 50-0552.  
☒ Any filing fee under 37 C.F.R. 1.16 for the presentation of additional claims which are not paid by check submitted herewith.  
☒ Any patent application processing fees under 37 C.F.R. 1.17.  
☒ Any petition fees for extension under 37 C.F.R. 1.136 which are not paid by check submitted herewith, and it is hereby requested that this be a petition for an automatic extension of time under 37 CFR 1.136.

  
 Erik R. Swanson, Reg. No. 40,833  
 DAVIDSON, DAVIDSON & KAPPEL, LLC  
 485 Seventh Avenue, 14<sup>th</sup> Floor  
 New York, New York 10018  
 Tel: (212) 736-1940  
 Fax: (212) 736-2427

I hereby certify that the documents referred to as attached therein and/or fee are being deposited with the United States Postal Service as "first class mail" with sufficient postage in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" on 01/31/05.  
 DAVIDSON, DAVIDSON & KAPPEL, LLC

BY:   
 Oliver Platz



2/21  
JAK

520.1007

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Re: Application of: **Tobias MARTIN et al.**

Serial No.: 10/049,385 Confirmation No.: 3809

Filed: 06/19/2002

For: **METHOD FOR ESTABLISHING A COMMON KEY  
FOR A GROUP OF AT LEAST THREE  
SUBSCRIBERS**

Examiner: (not yet known)

Art Unit: 2121

Customer No.: 23280

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

January 27, 2005

**SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT**

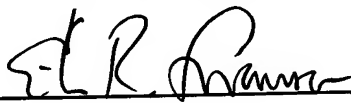
Sir:

In accordance with the provisions of 37 C.F.R. § 1.97, Applicants hereby make of record the documents listed on the accompanying Form PTO-1449 (1 page) for consideration by the Examiner in connection with the examination of the above-identified patent application. While the references are being submitted herewith, some or all of the references may not constitute prior art under the U.S. patent laws.

This Information Disclosure Statement is filed under 37 C.F.R. §1.97 (b), before the mailing date of a First Office Action, therefore no fee is believed due. If any additional fees are deemed to be due at this time, the Assistant Commissioner is authorized to charge payment of the same to Deposit Account No. 50-0552.

It is respectfully requested that the references cited in the accompanying PTO-1449 form be considered and made of record. It is respectfully submitted that the pending claims are patentable over all of the references made of record at this time.

Respectfully Submitted,  
DAVIDSON, DAVIDSON & KAPPEL, LLC

By:   
Erik R. Swanson  
Reg. No. 40,833

Davidson, Davidson & Kappel, LLC  
485 Seventh Avenue, 14th Floor  
New York, New York 10018  
(212) 736-1940

FORM PTO-1449  
(REV. 7-80)U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICE

ATTY DOCKET NO.

520.1007

APPLICATION NO

10/049,385

APPLICANT

Tobias MARTIN et al.

FILING DATE

06/19/2002

GROUP

2121

## LIST OF PRIOR ART CITED BY APPLICANT

(Use several sheets if necessary)



## U.S. PATENT DOCUMENTS

*EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE IF APPROPRIATE
	A01					
	A02					
	A03					
	A04					
	A05					
	A06					
	A07					
	A08					
	A09					

## FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLATION	
						YES	NO
	A10						
	A11						
	A12						
	A13						
	A14						

## OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

A15	W. DIFFIE et al., "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976, pp. 644-654	
A16	Internet Engineering Task Force Request for Comments 2412 (IETF RFC 2412): The Oakley Key Determination Protocol, The Internet Society, Network Working Group, H. Orman, November 1998, pp. 1-55	
A17	M. STEINER et al., "Diffie-Hellman Key Distribution Extended to Group Communication", 3 <sup>rd</sup> ACM Conference on Computer and Communications Security, March 14-16, 1996, New Delhi, India, pp. 31-37	
A18	M. BURMESTER et al., "Efficient and Secure Conference-Key Distribution", Security Protocols International Workshop, Cambridge, United Kingdom, Proceedings, M. Lomas, Ed., April 10-12, 1996, pp. 119-129	
A19	T. ELGAMAL, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, Vol. IT-31, No. 4, July 1985, pp. 469-472	
A20	M. BURMESTER et al., "A Secure and Efficient Conference Key Distribution System", Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994, pp. 275-286	

EXAMINER

DATE CONSIDERED

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.